News Release

報道関係各位

2024 年 3 月 19 日
トビラシステムズ株式会社

トビラシステムズ、フィッシング詐欺のリアルタイム観測サイト「詐欺 SMS モニター」の公開継続を決定

～サイバーセキュリティ月間中に観測した詐欺 SMS の調査レポートも公開～

特殊詐欺やフィッシング詐欺の対策サービスを提供するトビラシステムズ株式会社（本社：愛知県名古屋市、以下「トビラシステムズ」）は、内閣サイバーセキュリティセンター（NISC）が推進する「サイバーセキュリティ月間（2 月 1 日～3 月 18 日）」の関連行事として期間限定で、詐欺 SMS の検知状況をリアルタイムに観測し可視化する特設サイト「詐欺 SMS モニター」を公開しております。

この「詐欺 SMS モニター」について、サイバーセキュリティ月間の終了後も、引き続き公開を継続することを決定いたしましたので、お知らせいたします。

あわせて、サイバーセキュリティ月間中に観測した詐欺 SMS についてまとめた調査レポートも公開いたします。

■「詐欺 SMS モニター」公開継続の背景

「詐欺 SMS モニター」は、トビラシステムズの「迷惑情報データベース」に日々蓄積される調査・分析データを活用し、**詐欺 SMS のリアルタイム発生状況**や**最新のトレンド文面**などをわかりやすく可視化した特設サイトです。2 月 1 日～3 月 18 日の「サイバーセキュリティ月間」に、サイバーセキュリティへの関心を高め、理解を深めていただくことを目的として期間限定で公開いたしました。

しかしながら、特殊詐欺やフィッシング詐欺の被害抑止に向けた継続的な注意喚起や、詐欺 SMS 対策に関する認知拡大の必要性などを考慮し、サイバーセキュリティ月間終了後も引き続き「詐欺 SMS モニター」の公開を継続することを決定いたしました。

手口が多様化・巧妙化する詐欺 SMS の対策に「詐欺 SMS モニター」を引き続きご活用いただき、被害の未然防止にお役立てください。

■「詐欺 SMS モニター」の便利な使い方

◉「詐欺 SMS モニター」をスマートフォンのホーム画面に追加、またはブックマーク（お気に入り）に登録し、不審な SMS を受信したら随時チェックする
◉詐欺 SMS 検知グラフを見て、詐欺 SMS に特に注意すべき時間帯をチェックする
◉詐欺 SMS ギャラリーの投稿機能を使って、X のフォロワーに注意喚起する
◉詐欺 SMS に不安を感じている人や、スマートフォンの利用に慣れていない人に、詐欺 SMS の豆知識を伝え、安全なスマートフォン利用に役立ててもらう

・詐欺 SMS モニター
https://smon.tobila.com/

・X（旧 Twitter）アカウント
https://twitter.com/tobila_sms

■【調査レポート】直近の詐欺 SMS 検知状況を公開

「詐欺 SMS モニター」では、トビラシステムズの調査をもとに、詐欺 SMS の検知状況をリアルタイムに可視化するグラフや、Android マルウェア感染端末台数の表示、最新の詐欺 SMS 文面などを公開しています。

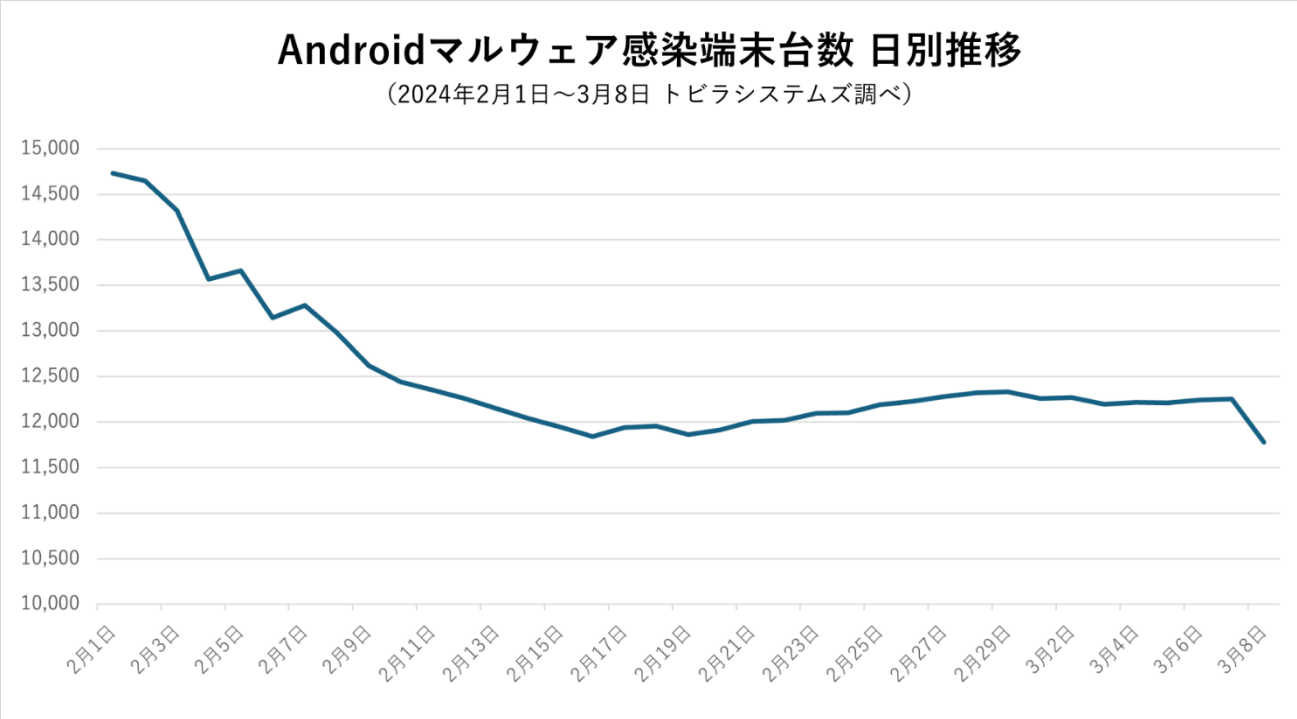
これらの検知状況を含め、サイバーセキュリティ月間中にトビラシステムズの調査で確認された直近の詐欺 SMS の動向について、以下に調査レポートを公開いたします。

○マルウェア感染端末台数は 12,000 台前後で推移

詐欺 SMS が増加している大きな要因に、**スマートフォンのマルウェア（不正アプリ）感染**が挙げられます。マルウェアに感染した端末は、連絡先など端末内の情報を悪用されたり、犯罪グループのサーバーから送られる指令に従って大量の詐欺 SMS をばらまき送信する**“踏み台”**として悪用されたりするおそれがあります。

トビラシステムズの調査では、2 月初旬はマルウェア感染端末が 14,000 台以上確認されていましたが、2 月中旬にかけて 12,000 台前後まで減少し、その後は横ばいで推移しています。

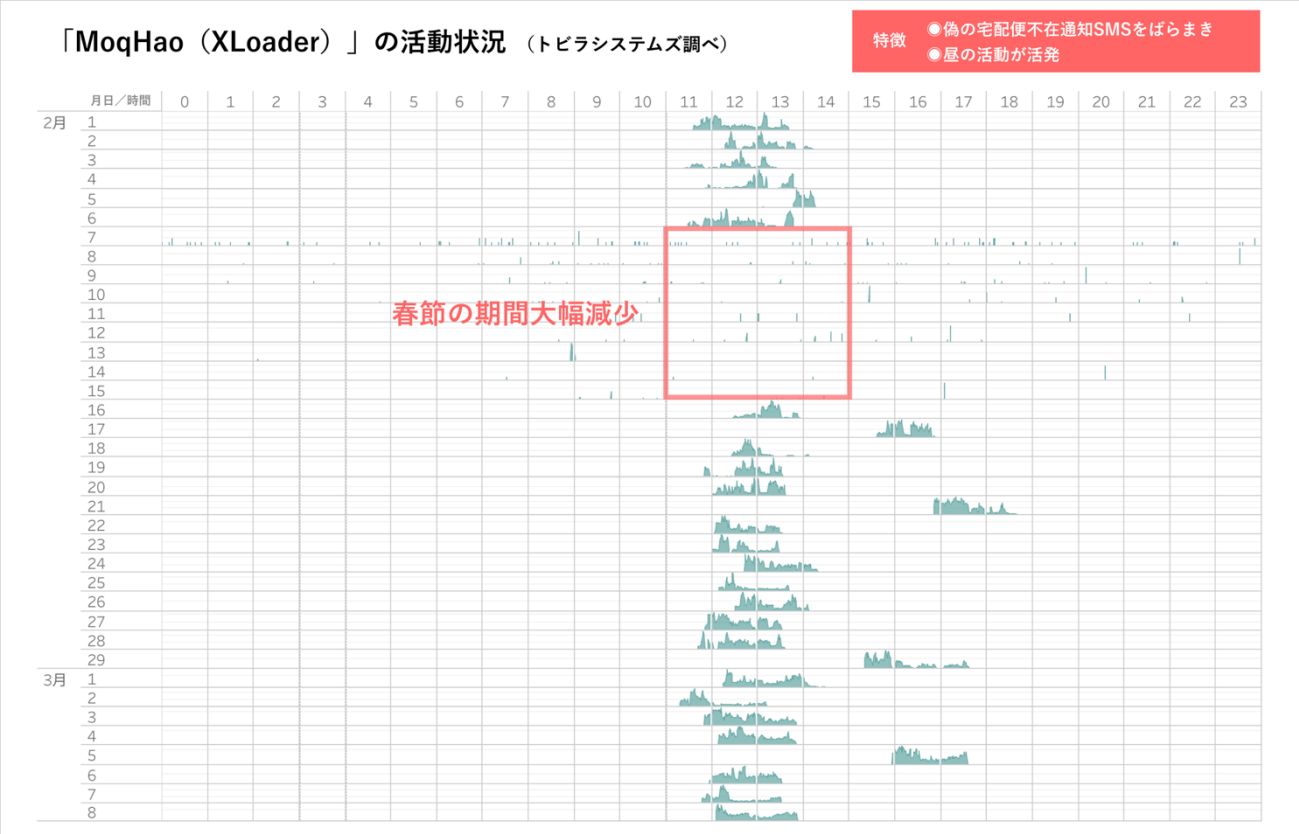
マルウェア感染端末台数が増加すると、詐欺 SMS のばらまき送信の活動も増加する可能性があり、引き続き注意が必要です。



○２大ばらまき送信型マルウェアの動向、偽の宅配便不在通知は春節に大幅減少

被害者の端末から詐欺 SMS を大量送信する“ばらまき型”のマルウェアは、大きく分けて２種類確認されています。以下、それぞれのマルウェアの活動や特徴について解説します。

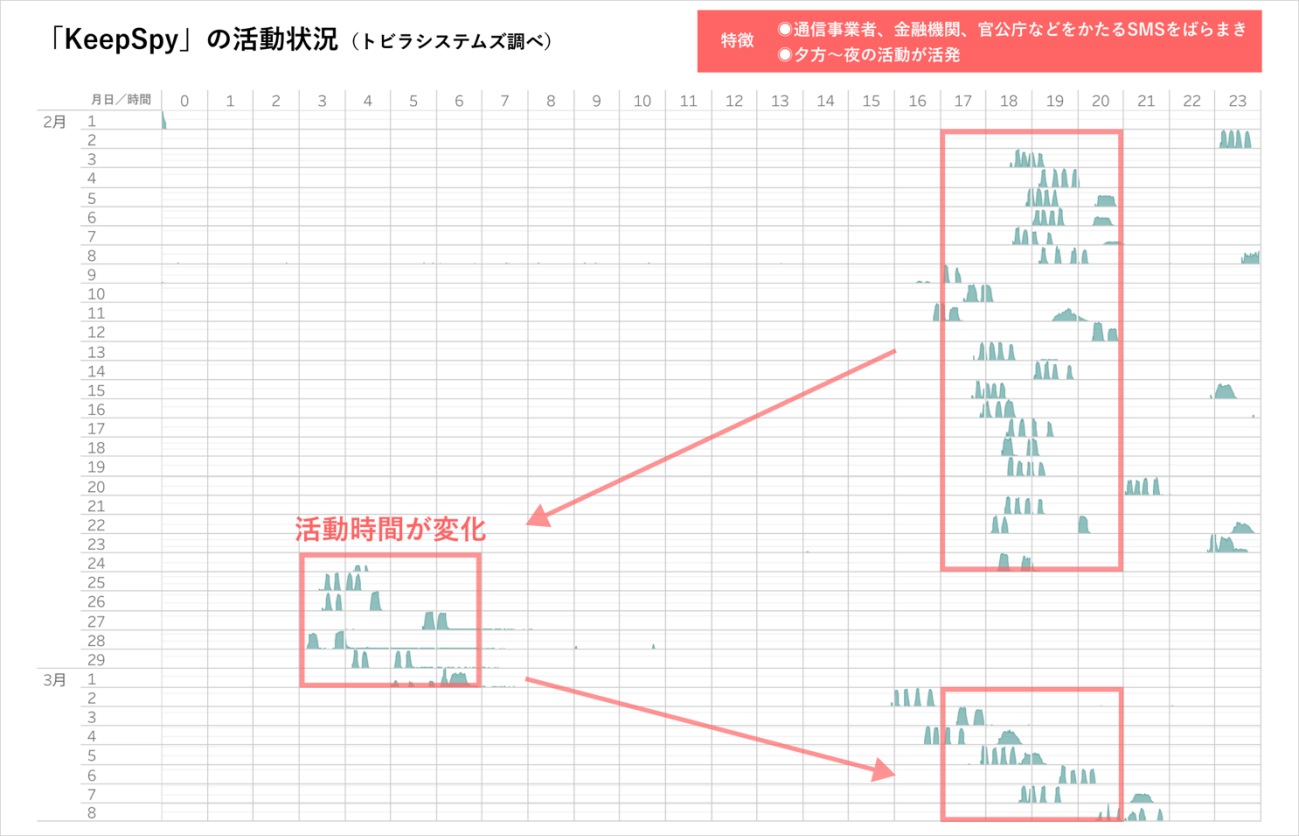
（１） マルウェア「MoqHao（XLoader）」



通称「MoqHao（XLoader）」と呼ばれるマルウェアは、これまでの調査で、主に**偽の宅配便不在通知 SMS** をばらまき送信する傾向が確認されています。また、**昼 12 時前後**に活動が活発化する特徴があります。

2024 年 2 月 7 日～15 日にかけては、当該マルウェア感染端末におけるばらまき送信の活動が大幅に減少しました。トビラシステムズの調査では例年、旧暦の正月**「春節」**に、宅配便不在通知を装う SMS が大幅に減少し、春節が明けると元の水準まで一気に戻る動きが確認されています。「MoqHao（XLoader）」に対してばらまき送信の指令を送る犯罪グループで、今年の春節の期間（2024 年 2 月 10 日～2 月 17 日）周辺に活動が大きく減少したと推測されます。

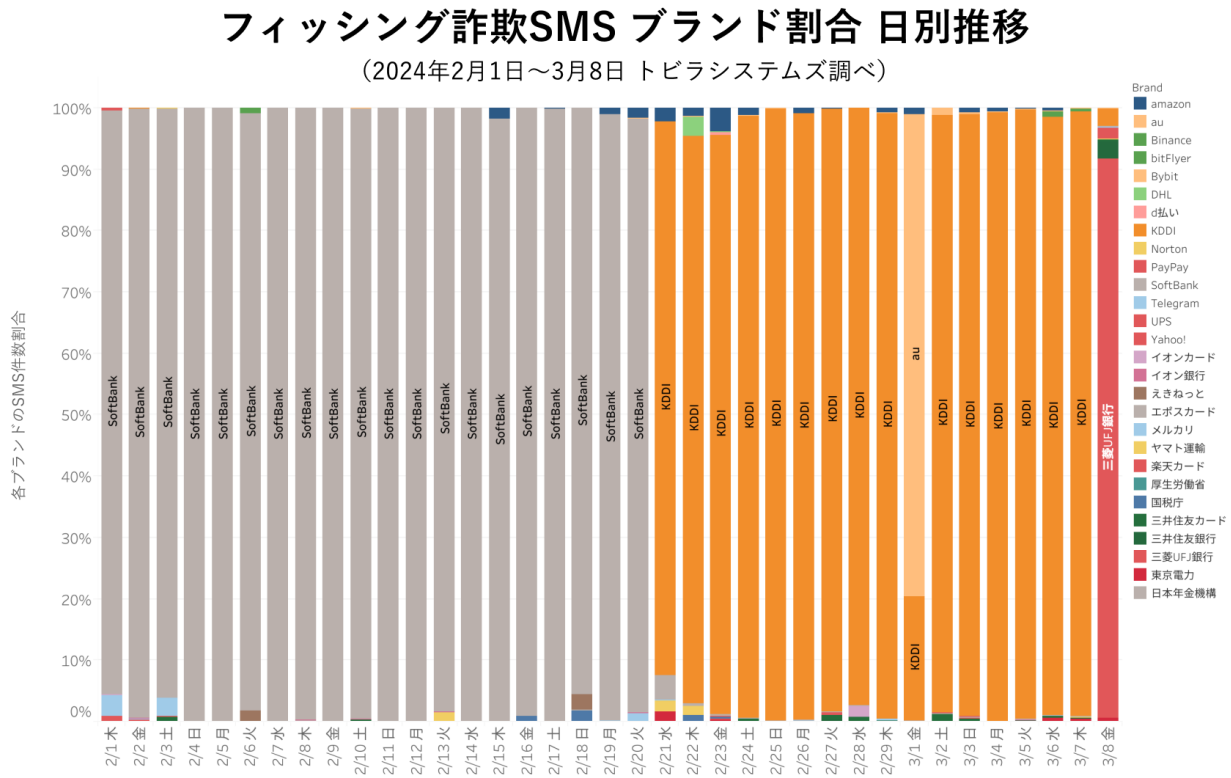
（2） マルウェア「KeepSpy」



通称「KeepSpy」と呼ばれるマルウェアは、これまでの調査で、**通信事業者や金融機関、官公庁**など様々な事業者をかたる SMS をばらまき送信する傾向が確認されています。また、**夜 19 時前後**に活動が活発化する特徴があります。なお、2 月の下旬には、未明～早朝の時間帯に活動が活発化した日も確認されました。

○ブランド別では通信事業者２社をかたる SMS が顕著

実在する企業やブランドの名前をかたる詐欺 SMS について、2 月～3 月上旬は主に通信事業者をかたる手口がトレンドとなりました。2 月 1 日～2 月 20 日は「**SoftBank**」、2 月 21 日～3 月 7 日は「**KDDI（au）**」をかたる文面が目立ちました。また、3 月 8 日以降は「**三菱 UFJ 銀行**」にトレンドが切り替わりました。



※特定のブランド名を記載しない宅配便不在通知など、文面にブランド名の記載がないSMSを除く。

＜参考資料＞

・ソフトバンク発表　注意喚起

https://www.softbank.jp/mobile/info/personal/news/support/20221129a/

・au サポート　よくあるご質問

https://www.au.com/support/faq/detail/61/a00000000161/

・三菱 UFJ 銀行発表　注意喚起

https://www.bk.mufg.jp/emeg/10_1332.html

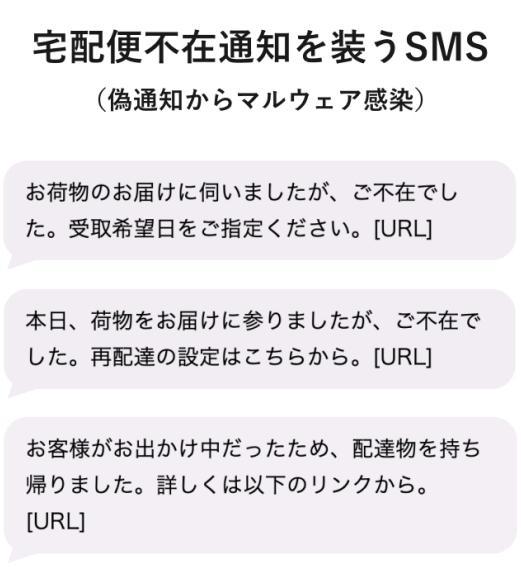
〇詐欺 SMS と偽サイトの事例

トビラシステムズの調査で確認された詐欺 SMS と偽サイトの事例を一部ご紹介します。

・偽通知からマルウェア感染する例

詐欺 SMS の URL にアクセスすると、ブラウザのアップデートを装う**偽通知**が表示される場合があります。指示に従って操作を行うと、端末がマルウェアに感染し、犯罪グループの遠隔操作によって詐欺 SMS をばらまき送信する“踏み台”として悪用されるおそれがあります。

偽通知からマルウェア感染に誘導する手口は、**宅配便不在通知を装う詐欺 SMS** で多く確認されています。



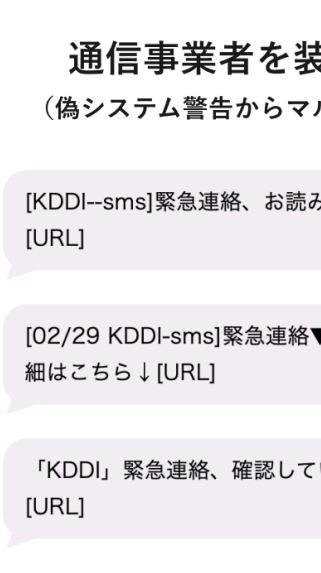
詐欺SMSの文例

ブラウザのアップデートを装う偽通知
指示に従い操作すると不正アプリに感染

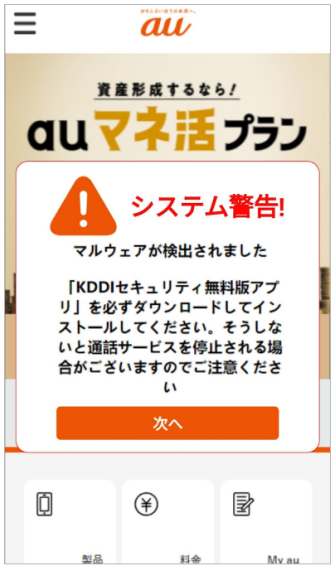
・偽のシステム警告からマルウェア感染する例

詐欺 SMS の URL にアクセスすると、**偽のシステム警告**が表示される場合があります。「マルウェアが検出された」「このアプリをインストールしないと通話サービスが停止される」などと不安をあおってセキュリティアプリのインストールを促しますが、実際にはマルウェア（不正アプリ）をインストールさせる手口です。

偽のシステム警告からマルウェア感染に誘導する手口は、**通信事業者を装う詐欺 SMS** で多く確認されています。



詐欺SMSの文例

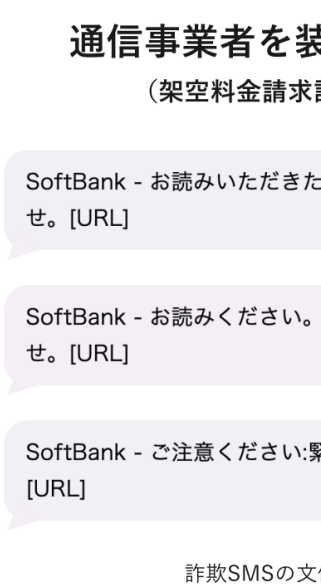


「このアプリをインストールしないと通話サービスが停止する」と脅し、不正アプリをインストールさせる

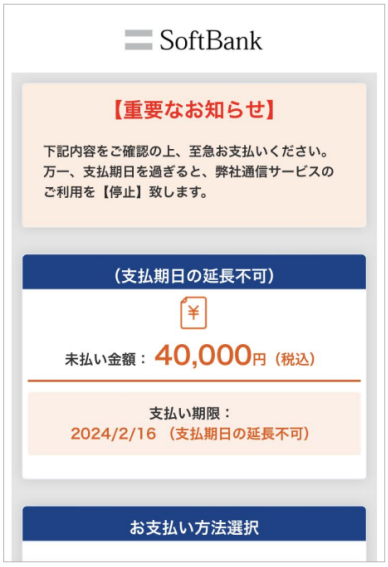
・架空料金請求の偽サイトに誘導する例

詐欺 SMS の URL にアクセスすると、**架空料金の支払い**を求める偽サイトが表示される場合があります。「未納料金がある」「支払わないとサービスを停止する」などと不安をあおり、プリペイドカードの購入等によって架空料金を支払わせる手口です。

架空料金請求の偽サイトに誘導する手口は、**通信事業者**や**官公庁**などを装う様々な詐欺 SMS で確認されています。



詐欺SMSの文例



「支払わなければ通信サービスを停止する」と脅し、架空の未納料金を請求

○詐欺 SMS の対策

詐欺 SMS の被害にあわないために、以下の対策を心がけてください。

◉身に覚えのないメールや SMS が届いた場合、文面に添付された URL に触らない
◉日頃利用するサービスは、公式アプリやブックマークしたサイトから情報を確認
◉迷惑 SMS 対策サービスを活用し、フィッシング詐欺などの不審な SMS を自動で遮断

■トビラシステムズについて

テクノロジーで社会課題の解決を目指し、特殊詐欺やフィッシング詐欺、グレーゾーン犯罪撲滅のためのサービスを提供しています。詐欺電話・詐欺 SMS 等の情報を収集・調査してデータベースを構築し、自動でフィルタリングする「迷惑情報フィルタサービス」は、固定電話、モバイル、ビジネス向けに展開し月間約 1,500 万人にご利用いただいています。

公式サイト：
https://tobila.com/

＜本件に関する報道関係のお問い合わせ先＞
トビラシステムズ株式会社
〒460-0003 愛知県名古屋市中区錦２丁目 5-12 パシフィックスクエア名古屋錦７F
担当：管理部 広報 岩渕
TEL：050-3646-6670（直通）
FAX：052-253-7692
URL：https://tobila.com/